

To: HIPAA Division Liaisons and Contract Managers
From: Geralyn Driscoll
Re: HIPAA Business Associate Agreements
Date: March 19, 2003

You received an e-mail regarding Business Associate Agreements from Sally Klein on February 7, 2003. Each DPHHS Division must identify what, if any, work is performed for the Division by a Business Associate. The Montana Medicaid HIPAA Assessment done by ACS/Consultec and Birch & Davis may be of some help to you in the identification process.

Sally's e-mail also informed you that the Division Liaison and the Contract Manager would be responsible for coordinating each Division's efforts to identify its Business Associates. The converse of this task – determining whether the Department should agree it is another entity's Business Associate and sign Business Associate Agreements when requested – will also be coordinated through you.

This memo is intended to provide you with some background information to assist you with these tasks. The memo has three parts. Part 1. reviews identifying Business Associates and gives you a check list to use if you want. Part 2. reviews the process of determining whether the Department is, in fact, the Business Associate of another entity and gives you a form letter you can use if you want to notify a requestor that the Department is not signing a requested Business Associate Agreement. Part 3. reviews drafting Business Associate Agreements. All three steps are "works-in-process" as the April 14, 2003 deadline approaches. If you have any suggestions or have questions about a specific contract you can contact me at 444-5331 or 723-3879.

April 14, 2003 is the compliance date for HIPAA but there is a transition period for Business Associate Agreements. If the Department had an existing contract with a Business Associate prior to October 15, 2002, it may operate under that contract up to April 14, 2004. During our March 4th meeting we suggested that you begin your review of contracts with an effective date of 9/1/02, however, contracts entered into after October 15, 2002 and up to April 14, 2003 and are identified during your review process as a Business Associate must have a Business Associate Agreement by April 14, 2003. As discussed in Part 3., there will be a Business Associate Agreement contract addendum that can be used for contracts entered into between October 15, 2002, and April 14, 2003. For contracts after that date, the original contract should included Business Associate Agreement language if appropriate.

1. Identifying Business Associates (Suggested worksheet - see Attachment A)

What is the purpose of a Business Associate Agreement?

All of DPHHS is a 'Covered Entity' as that term is defined in the HIPAA regulations. That means the HIPAA privacy requirements related to Protected Health Information ("PHI")

must be followed throughout the Department. One requirement is that if the Covered Entity, i.e. DPHHS, discloses Individually Identifiable Health Information (“IIHI”) to a contractor, the contractor must provide written “satisfactory assurances” that it will appropriately safeguard the information it receives from or creates for DPHHS. The written, satisfactory assurances is the Business Associate Agreement.

What is a Business Associate?

A business associate is a person or legal entity (not an employee of DPHHS) who acts on behalf of DPHHS to perform a function or activity that involves the use or disclosure of IIHI.

If the contract function does not require the use or disclosure of IIHI the entity is NOT a Business Associate. If the contract function involves a limited, incidental use or disclosure of IIHI (a secondary use or disclosure that cannot be reasonably prevented, is limited in nature and occurs as a result of another use) the entity is also NOT a Business Associate.

There are some limited exceptions to the Business Associate requirement. Probably the most important exception to understand is the Healthcare Provider exception. If a Healthcare Provider discloses PHI to or receives it from DPHHS for payment purposes, no Business Associate Agreement is needed. Both the contractor and DPHHS are acting on their own behalf as Covered Entities, not as Business Associates.

You should carefully review any contracts that have the following purposes:

data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, legal, actuarial, accounting, consulting, data aggregation management, administrative, accreditation, or financial services.

These are the functions listed in the HIPAA privacy rules as examples of business associates. If there is any potential that IIHI will be shared there must be a Business Associate Agreement.

What is IIHI?

The HIPAA regs define at least three kinds of information, – Health Information (“HI”), IIHI, and PHI. PHI is a subset of IIHI, which, in turn, is a subset of HI. (The definitions in regulations of HI, IIHI, PHI and Business Associate are attached.)

HI is information in any form that is created or received by a:

Healthcare Provider, health plan, public health authority, employer, life insurer, school or university or health care clearinghouse and relates to:

the past, present, or future physical or mental health or condition of an individual;
the provision of health care to an individual; or
the past, present, or future payment for the provision of health care to an individual.

The Medicaid program is, by definition, a health plan, that receives and creates HI. The entire Department, however, not the Medicaid program, is the Covered Entity (as that term is defined in the HIPAA regulations), therefore all DPHHS Divisions must comply with the HIPAA privacy requirements regarding HI.

IIHI is a subset of health information that:

is collected from an individual;
either identifies the individual; or
there is a reasonable basis to believe the information can be used to identify the individual.

It is important for Divisions to note the “created or received” language. A Division that does not create HI or have a “Designated Record Set” as that term is defined in 164.501 may, nevertheless, receive IIHI. That Division must have Business Associate Agreement with a contractor to whom the Division discloses IIHI. As DPHHS implements HIPAA, employees may need assistance in coming to understand this point.

PHI is a subset of IIHI. It is Individually Identifiable Health Information, transmitted or maintained in any medium, except IIHI in education records and Covered Entity employment records.

2. To sign or not to sign a Business Associate Agreement from a third party requestor. (Form letter to be adapted for use when a requested Business Associate Agreement is not signed - see Attachment B.)

DPHHS should only sign Business Associate Agreements if it concurs in the third part requestor’s position that the Department is a Business Associate. The analysis is the same as in 1. above, except you review the request from the perspective of whether the Department acts on the requestor’s behalf to perform a function or activity that involves the use or disclosure of IIHI.

Requests for signed Business Associate Agreements will increase as we get closer to April 14, 2002. If you determine that the requested Business Associate Agreement should not be signed, you should send the attached letter to the requestor. If you determine that the Business Associate should be signed, you should forward the agreement to the Division Administrator with your explanation of why the agreement should be signed. As of the date of this memo, only Division Administrators should sign Business Associate Agreements. As the process evolves and we all become more familiar with Business Associate Agreement requests this process may be modified.

3. Business Associate Agreement Language

A suggested form for contract addendums that can be used for contracts entered into between October 15, 2002, and April 14, 2003. This will be placed on the shared drive for you to use

with Business Associates that you identify and that have entered into a contract with DPHHS since October 15, 2002. This should be on the shared directory by the end of this month.

For a Business Associate you identify with whom DPHHS contracts after April 14, 2003 there will be specific language included in the contract manual that applies to a Business Associate. After April 14, 2003 the original contract with a Business Associate should either include Business Associate Agreement language in the body of the contract or have a Business Associate Agreement as an addendum. I intend to have the contract manual updated by the end of March.

All contracts dated after April 14, 2003 will include a reference to HIPAA in the certification of compliance language. This will also be included in the contract manual by the end of March.